Amendments to the Claims:

The listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claims 1.-22. (Cancelled)

Claim 23. (New) A method for loading an application program into a program memory of a microprocessor system having a processor bus that is connected to at least one microprocessor; at least one program memory with a boot sector, a flash boot loader, an electrically erasable and programmable memory and a read-write memory; and at least one system interface; said method comprising:

producing an authentication code for the application program;

reading in the authentication code and the current application program, via the system interface; and

before a read-in current application program is actuated, checking the authentication code; wherein,

the authentication code is calculated in a secured area by concatenating the application program with a first secret data string and calculating a hash value from the concatenated application program;

the hash value is read into the microprocessor system, via the system interface, as an authentication code;

a second, identical, secret data string is stored in the microprocessor system;

the read-in application program is concatenated with the second secret data string in the microprocessor system; and

a hash value is calculated by the read-in, concatenated application program in the microprocessor and is compared with the transmitted authentication code.

Claim 24. (New) The method as claimed in Claim 23, wherein:

the application program is concatenated with the first secret data string in the microprocessor at the start of the program and at the end of the program, both in the secured area and during the authenticity checking;

a hash value is calculated using the application program which is concatenated at both ends; and

the hash value is read in as an authentication code at the system interface.

Claim 25. (New) The method as claimed in Claim 23, wherein:

the application program is initially concatenated with the first secret data string either at the start of the program or at the end of the program;

in a following step, a first hash value is calculated in the secured area by using the application program which is concatenated at one end;

in a subsequent step, the first hash value is concatenated with a first secret data string at one end;

in a still further step, a second hash value is calculated by the combination of a first hash value and the first secret data string, and said second hash value is read in as an authentication code at the system interface;

a second, identical, secret data string is stored in the microprocessor system and the steps carried out in the secured area are repeated with the

original application program in the same sequence using said second secret data string in the microprocessor; and

the hash value which is calculated in the microprocessor is compared with the hash value which is read in at the system interface.

Claim 26. (New) The method as claimed in Claim 25, wherein the authentication code is transferred together with the application program.

Claim 27. (New) The method as claimed in Claim 25, wherein the authentication code is transferred separately from the application program.

Claim 28. (New) The method as claimed in Claim 27, wherein:

the application program is stored and distributed in a memory medium; and

the authentication code is transmitted to the system interface from the secured area by means of data transmission.

Claim 29. (New) The method as claimed in Claim 26, wherein the application program and the authentication code are transmitted to the system interface from the secured area by data transmission.

Claim 30. (New) The method as claimed in Claim 29, wherein the authentication code is read into a control unit of a motor vehicle via the diagnostic interface.

Claim 31. (New) The method as claimed in Claim 30, wherein if a read-in authentication code and a hash value calculated in the microprocessor correspond, the associated application program is provided with an identifier as a valid application program.

Claim 32. (New) The method as claimed in Claim 31, wherein flashware meta information is included in the authentication code.

Claim 33. (New) The method as claimed in Claim 32, wherein the authentication code is used to selectively download the application program into various control units.

Claim 34. (New) A method for safeguarding authenticity of flashware for a control unit of a motor vehicle in which an application program is stored in a program memory; said method comprising:

in a secured area, concatenating the application program with a first secret data string, and calculating a hash value using the concatenated application program;

reading the hash value into the control unit as an authentication code;

storing a second, identical, secret data string in the control unit;

concatenating application program with the second secret data string in the control unit;

calculating a second hash value using the concatenated application program in the control unit; and

comparing the calculated second hash value with the transmitted authentication code.

Claim 35. (New) The method as claimed in Claim 34, wherein:

the application program is concatenated with the first secret data string in the control unit at the start of the program and at the end of the program, both in the secured area and during the authentication checking;

a hash value is calculated using the application program which is concatenated at both ends; and

the hash value is read in as an authentication code at the system interface.

Claim 36. (New) The method as claimed in Claim 34, wherein:

the application program is initially concatenated with the first secret data string either at the start of the program or at the end of the program;

in a following step, a first hash value is calculated in the secured area using the application program which is concatenated at one end;

in a subsequent step, the first hash value is concatenated with a first secret data string at one end;

in a still further step, a second hash value is calculated by the combination of a first hash value and the first secret data string, and said second hash value is read in as an authentication code at the system interface;

a second, identical, secret data string is stored in the control unit and the steps carried out in the secured area are repeated with the original application program in the same sequence using said data string in the control unit; and

the hash value which is calculated in the control unit is compared with the hash value which is read in at the system interface.

Claim 37. (New) The method as claimed in Claims 36, wherein the authentication code is transferred together with the application program.

Claim 38. (New) The method as claimed in Claim 36, wherein the authentication code is transferred separately from the application program.

Claim 39. (New) The method as claimed in Claim 38, wherein the application program is stored and distributed in a memory medium; and

the authentication code is transmitted to the system interface from the secured area by means of data transmission.

Claim 40. (New) The method as claimed in Claim 37, wherein the application program and the authentication code are transmitted to the system interface from the secured area by means of data transmission.

Claim 41. (New) The method as claimed in Claim 40, wherein the authentication code is read into a control unit of a motor vehicle via the diagnostic interface.

Claim 42. (New) The method as claimed in Claim 41, wherein if a read-in authentication code and a hash value calculated in the control unit correspond, the associated application program is provided with an identifier as a valid application program.

Claim 43. (New) The method as claimed in Claim 42, wherein flashware meta information is included in the authentication code.

Claim 44. (New) The method as claimed in Claim 43, wherein the authentication code is used to selectively download the application program into various control units.